PCS 6166 - INTERNATIONAL DATA PROTECTION AND CYBERSECURITY LAW

Part Four – Comparative National Approaches

Cybersecurity

Cybersecurity – Canadian Regulations

- **PIPEDA**
  - **4.7**. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
    - **4.7.1**. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
    - **4.7.2**. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. …
    - **4.7.3**. The methods of protection should include [physical measures, organizational measures, and technological measures.]
    - **4.7.4**. Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
    - **4.7.5**. Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information
- **Privacy Act**
  - No explicit requirements to safeguard personal information.
- **Specific Industry Guidelines** (example):
  - Office of the Superintendent of Financial Institutions
    - Applies to Federally Regulated Financial Institutions
    - Includes: Technology and Cyber Risk Management guidelines (updated November 2021); incident reporting guidelines (updated August 2021); cyber security self-assessment (updated August 2021)

Cybersecurity – Deterrence Approach

- **2001**: Council of Europe Convention on Cybercrime (aka "Budapest Convention")
  - Canada is one of 65 parties to the Convention
  - "Each Party shall adopt such legislative measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, …"
    - Article 2: Access to a computer system without right (**Illegal access**)
    - Article 3: Interception without right of non-public transmissions of computer data (**Illegal interception**)
    - Article 4: Damaging, deletion, deterioration, alteration or suppression of computer data without right (**Data interference**)
    - Article 5: Serious hindering without right of the functioning of a computer system (**System interference**)
    - Article 6: Production, sale, making available, etc. of devices or passwords to enable Articles 2-5 . (**Misuse of devices**)
  - Also sets out computer-related offences (fraud, forgery); content-related offences (child pornography); copyright-related offences

Cybersecurity – Deterrence Approach

Convention on Cybersecurity / Budapest Convention, cont'd

- Benefits of the Convention (per July 2020 report)
  - All 65 parties (~1/3 of world) to Budapest Convention have reformed legislation; 153 UN member states have used convention as a guideline or source for reforms
  - Establishes procedures pertaining to mutual assistance.
    - Article 25.1: The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
      - Includes procedures for assistance *in absence of* international agreements; expedited preservation; expedited disclosure of preserved evidence; accessing of stored data, collection of real-time data, etc.
  - Establishes Cybercrime Convention Committee and "24/7 Contact Points" – networks of practitioners who can share information and call upon one another.
- "Experience after almost twenty years since its opening for signature shows that there are no disadvantages in joining this treaty."

Cybersecurity – Deterrence Approach

- Next up: A potential UN Convention on Cybercrime
- Resolution 74/247 (December 2019) established an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention
  - Relatively controversial / divisive resolution: 88 in favour; 58 opposed (including Canada); 34 abstentions
  - Sponsors: Russia, Belarus, Cambodia, China, North Korea, Myanmar, Nicaragua, Venezuela
- Resolution 75/282 (May 2021) decides that a draft convention on cybercrime will be presented at the 78th session of the General Assembly (Sept. '23 – Sept. '24)

Some response:

- Human Rights Watch: "Cybercrime is dangerous, but a new UN treaty could be worse for rights" (August 13, 2021)
- Key issues:
  - Who determines the meaning of "cybercrime"?
  - What additional powers are granted to law enforcement agencies?

Cybersecurity – Appropriate Protections Approach

PIPEDA

Principle 4.7. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

GDPR:

Article 5.1(f): Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 25.1 ("Data protection by design and by default"): Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures … to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Cybersecurity – Transparency Approach

Breach reporting

GDPR

> **Article 33.1**: In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority … unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
>
> **Article 34.1**: When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

- **Ransomware payment reporting**
  - For instance: Australia's Ransomware Action Plan
  - Proposed legislative reforms:
    - Introducing a specific mandatory ransomware incident reporting to the Australian Government
    - Introducing a stand-alone offence for all forms of cyber extortion
    - Introducing a stand-alone aggravated offence for cybercriminals seeking to target critical infrastructure
    - Modernising legislation to ensure that cybercriminals are held to account for their actions, and law enforcement is able to track and seize or freeze their ill-gotten gains

Cybersecurity – Government-centric Approach

- Consider: United States, President Biden's Executive Order on Improving the Nation's Cybersecurity (May 2021)
- Elements:
  - Removing barriers to sharing threat information
    - Particularly encourages sharing of information between government and private sector
  - Modernizing Federal Government cybersecurity
    - Includes adopting "Zero Trust Architecture", accelerating movement to secure cloud services
  - Enhancing software supply chain security
    - In essence, NIST is meant to issue standards, procedures and/or criteria for a wide range of practices that enhance the security of the software chain. This include: secure software development processes; trusted code supply chains; automated vulnerability monitoring; etc.
  - Establishing a cyber safety review board
  - Standardizing the Federal Government's playbook for responding to cybersecurity vulnerabilities and incidents
  - Improving detection of cybersecurity vulnerabilities and incidents on Federal Government networks
  - Improving the Federal Government's Investigative and Remediation Capabilities

Cybersecurity – High Risk Target Approach

- Consider: US Cybersecurity Requirements for Critical Pipeline Owners and Operators
- Directive 1 (May 2021)
  - Report cybersecurity incidents to the DHS
  - Designate a cybersecurity coordinator
  - Review their current activities against the Pipeline Cyber Asset Security Measures
- Directive 2 (July 2021 – redacted version available via Washington Post)
  - Implement specified cybersecurity mitigation measures;
  - Develop a cybersecurity contingency and recovery plan in the event of an incident;
  - Undergo an annual cybersecurity architecture design review

Cybersecurity – High Risk Target Approach

Consider: China's Regulations on the Security and Protection of Critical Information Infrastructure (summary)

- Came into force Sept. 1, 2021
- Applies to: "Important industries or fields", including communications, transportation, energy, water, finance, etc.
  - Also considers: importance of system for core business; level of harm in case of failure; impacts on other industries
- Note: The senior executive of CIIO is personally liable for the security and protection of the organization.

Responsibilities and Obligations of CII Operators

Building a robust network security system	Setting up a specialized security management system	Coordinating with regulatory authorities	Keeping oversight of third-party products and services
CII operators are required to establish a robust network security system and system of work responsibility. Responsibilities include: • Ensuring staffing, finances, and resources are invested into the system to keep it operational. • Ensuring CII is factored into the planning, building, and usage of the cybersecurity protection measures. • Ensuring a staff member from a specialized security management agency takes part in any decision-making processes related to cybersecurity or digitization.	CII operators are required to set up a dedicated security management mechanism. Responsibilities include: • Footing the operational costs and organizing staffing for the mechanism. • Conducting security background checks of the personnel in charge of the cybersecurity protection mechanism.	CII operators are required to maintain regular communication with regulatory authorities over issues of cybersecurity and network maintenance. Responsibilities include: • Promptly informing the relevant authorities of any major changes to the network infrastructure that may affect the company's designation as a CII operator. • Reporting any major issues or threats to cybersecurity to regulatory departments and the public security bureau. • Informing regulatory departments when conducting vulnerability assessments or penetration testing. • Reporting mergers, divisions, dissolutions, or any other changes to the company structure.	If a CII operator purchases internet products or services from a third-party vendor, them they must be responsible for: • Prioritizing the purchase of secure and trustworthy products and services. • Conducting security assessment of the services in accordance with cybersecurity regulations. • Signing security and confidentiality agreements with the service providers, clarifying the providers' technical support, security, and confidentiality responsibilities. • Supervising the providers' performance and fulfilment of responsibilities.

Source: China State Council

Cybersecurity – Sector-Specific Regulation

- Consider: Rwanda Cybersecurity Regulation N°010/R/CR-CSI/RURA/020 ("Regulation 10")

- Brief notes on Rwanda
  - Key organizations: National Cyber Security Authority (NCSA – also the Rwandan DPA); Rwanda Information Society Authority (RISA)
    - RISA has issued "Directives on Cyber Security for Network and Information Systems for all Public Insitutions"
  - Also has sectoral regulators, such as Rwanda Utilities Regulatory Authority (RURA, which oversees Regulation 10)
    - RURA oversees and licenses "public utilities", including telecommunications, broadcasting, ISPs, energy, water, transportation, etc.

- Regulation 10 applies to "all ICT infrastructure and services provided to the public"
- Purpose: To secure networks, their subscribers and the critical communication infrastructure to ensure the confidentiality, integrity and availability of networks and systems in Rwanda

Cybersecurity – Sector-Specific Regulation

Rwanda Cybersecurity Regulation, cont'd

- Licensee responsibilities are broad, and include:
  - "Implementing, operating, maintaining and monitoring the controls mentioned in this regulation and required international standards such as ISO/IEC 27001: 2013 or ISO/IEC 27011 as it may be amended from time to time"

Penalties:

- Failure to implement security measures: RWF 1M to 5M; continuous failure "shall incur additional sanctions that may lead to revocation of license"

- Sample text:
  - A comprehensive Information Security Management System (ISMS) must be implemented including the essential components hereunder:
    - (a) risk assessment;
    - (b) information security policies
    - (c) asset management
    - (d) access control
    - (e) communications and operations management
    - (f) configuration management;
    - (g) change management;
    - (h) incident management;
    - (i) secured application acquisition, development and maintenance;
    - (j) business continuity plan and disaster recovery plan;
    - (k) vulnerability assessment and audit;
    - (l) internal and external penetration testing by auditors approved by the regulatory authority;
    - (m) legal and regulatory compliance identifying, maintaining and monitoring;
    - (n) cryptographic algorithm management;
    - (o) human resources security; and
    - (p) backup management.

Cybersecurity – Sector-Specific International Standards

- Consider: UN Economic Commission for Europe (UNECE) WP.29 – World Forum for Harmonization of Vehicle Regulations
  - Active since 1958
- In 2020, WP.29 issues regulation for cyber security and cybersecurity management systems in vehicles
  - In force since January 2021, certification required for most vehicles sold here:

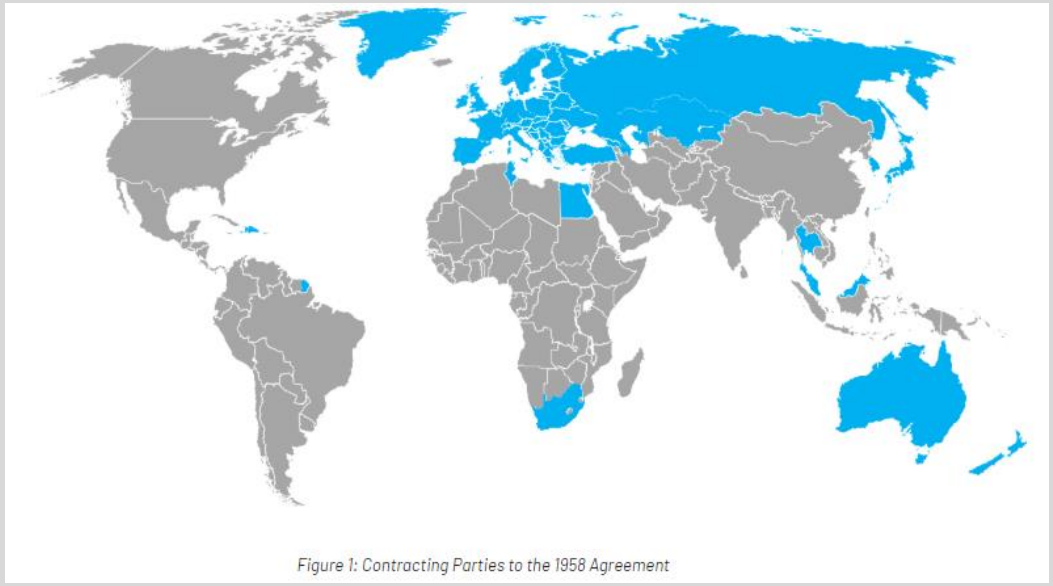


Figure 1: Contracting Parties to the 1958 Agreement

Cybersecurity – Sector-Specific International Standards

UNECE WP.29 Cybersecurity Regulations, cont'd.

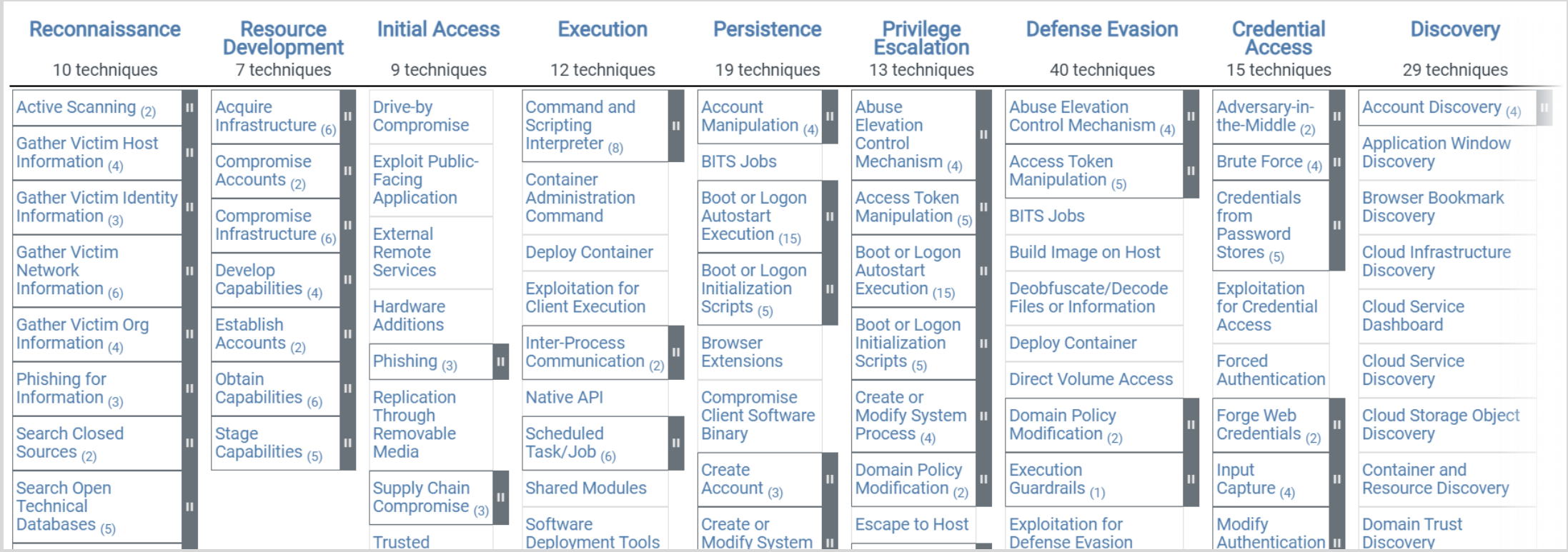
- 7.2.2: The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. …
- Annex 5:
  - Sets out types of attack impacts: safe operation of vehicle affects; vehicle functions stop working; data confidentiality breach; etc.
  - Lists potential vulnerabilities and attack methods (32 in total), corresponding mitigations (sample below)

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data

[Consider also ISO/SAE 21434:2021 – Road Vehicles – Cybersecurity Engineering]

Cybersecurity – Shared Knowledge

- Consider: [MITRE ATT&CK Matrix]



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Access Token Manipulation (5)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (15)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery
Search Open Technical Databases (5)		Trusted	Shared Modules	Create or Modify System	Escape to Host	Domain Policy Modification (2)	Modify Authentication	Container and Resource Discovery
			Software Deployment Tools			Execution Guardrails (1)		Domain Trust Discovery
						Exploitation for Defense Evasion		

Cybersecurity – Certification

Consider: EU Cybersecurity Act (April 2019)

[Side Note: EU also has the Directive on Security of Network and Information Systems]

- Strengthens (and makes permanent) the European Union Agency for Cybersecurity (ENISA)
- Sets out a framework for the establishment of European cybersecurity certification schemes
  - Each sheme should specify:
    a) the categories of products and services covered,
    b) the cybersecurity requirements, for example by reference to standards or technical specifications,
    c) the type of evaluation (e.g. self-assessment or third party evaluation), and
    d) the intended level of assurance (e.g. basic, substantial and/or high).

EUCC Scheme

- Based on the Common Criteria (ISO/IEC 15408) and the Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)

Methodology for Sectoral Cybersecurity Assessments

- In essence – a first step towards identifying the cybersecurity requirements of an industry, based on risk.

Personal Information and De-Identification

Regulating Non-Identifiable Data

Khaled El Emam and Mike Hintze: 10 Recommendations for Regulating Non-Identifiable Data

Principles

1. Reduce uncertainty.
2. Create incentives.
3. Recognize and calibrate the broad benefits of non-identifiable data.

Practices

4. Enable the creation of non-identifiable data without consent.
5. Clarify whether destroying original (identifiable) data is necessary.
6. Risks should be assessed for an anticipated adversary.
7. Define acceptable thresholds.
8. Require ethics review rather than regulate specific uses of non-identifiable data.
9. The data processing context and controls should be considered.
10. Define the consequences of re-identification attacks.

Key definitions

GDPR

- '**personal data**' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly …;
- '**pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Anonymous or anonymized information is defined less directly in Recital 26, as:

> "… information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

Canada

PIPEDA

> ***personal information*** means information about an identifiable individual**.**

C-11

> ***de-identify*** means to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.

Ontario

> "**de-identified information**" means information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information.
>
> **Anonymized information**: this Act does not apply to information [that] has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person.

Key Definitions: Personal Information

- Definition of "personal information" is often largely consistent.

Canada

PIPEDA / Privacy Act

"personal information means information about an identifiable individual …"

(see also OPC Interpretation Bulletin on Personal Information)

Gordon v. Canada: Information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information

Ontario Personal Health Information Protection Act (PHIPA)

"personal health information … means identifying information about an individual …"

EU

'**personal data**' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly …;

South Africa (a randomly chosen example)

"**personal information**" means information relating to an identifiable, living, natural person …

Key Definitions: Pseudonymization

GDPR

- "… personal data [that] can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures [to prevent re-identification]"

Bill 64:

- "For the purposes of this Act, personal information is de-identified if it no longer allows the person concerned to be directly identified;"

Ontario Privacy Reform White Paper:

- "de-identified information" means information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information.

Key Definitions: Anonymization

GDPR

- Recital 26: "… information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

Ontario Private Sector White Paper:

- **"**… information [that] has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person.

Quebec Bill 64:

- "information … is anonymized if it irreversibly no longer allows the person to be identified directly or indirectly. Information anonymized under this Act must be anonymized according to generally accepted best practices."

De-identification

- Specific thresholds may change, but in general this is the overall understanding.

- Likelihood of identifiability:

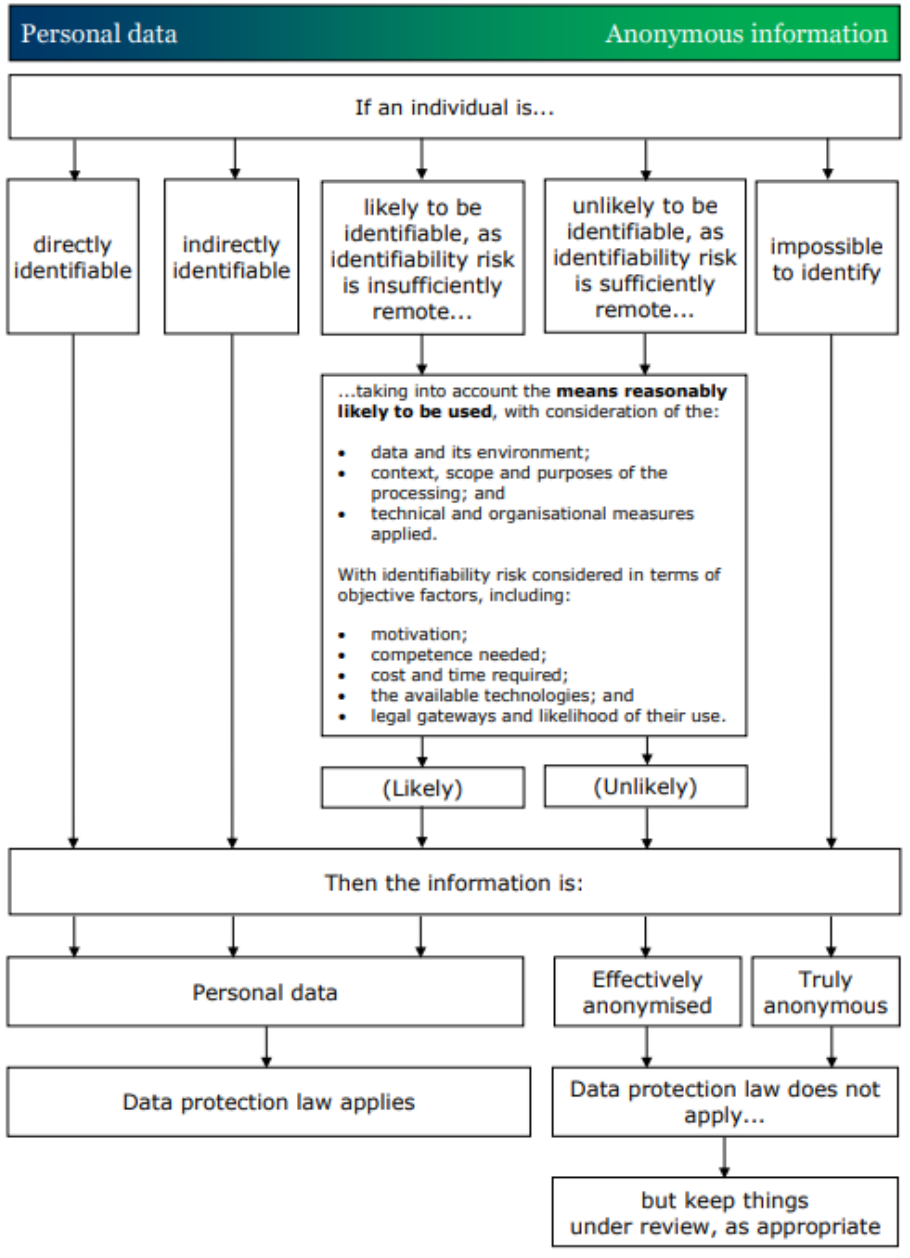
Probability re-identification attempt will occur

x

Probability a re-identification attempt will succeed

Source: UK Information Commissioner's Office, Draft anonymization, pseudonymization and privacy enhancing technologies guidance (October 2021)

Chapter 2: How do we ensure anonymization is effective?



De-Identification: Japan.

Japan: Act to Protect Personal Information

- 2015:
  - Introduces into law the concept of “anonymously processed information”, “anonymously processed information handling business operator” (Articles 36 - 39 - Japan DPA Guidance)
    - Includes disclosure to the public about what information has been anonymised; prohibitions against re-identification, etc.
- 2020:
  - Introduces “pseudonymously processed information” (and associated requirements for users – Articles 35-2 and 35-3)
    - Can use this information without consent, but cannot disclose or re-identify it.
  - Also introduces “personally referable data” - information relating to an individual which does not fall under personal information, pseudonymously processed information or anonymously processed information
    - Effectively, requires consent to disclose information that *is not* PI to the discloser, but *is* PI to the receiver

De-Identification: India.

Consider: Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019. (December 2021)

Key quotes:

1.15.8.3: The Committee observe that to define and restrict the new legislation only to personal data protection … is detrimental to privacy. The Bill is dealing with various kinds of data at various levels of security, and it is impossible to distinguish between personal data and non-personal data, when mass data is collected or transported. So, **the Committee opine that if privacy is the concern, non-personal data has also to be dealt with** in the Bill. … [We] cannot have two DPAs, one dealing with privacy and personal data and the other dealing with non-personal data.

1.15.8.4: … [Since] the DPA will handle both personal and non-personal data, any further policy/legal framework on non-personal data may be made a part of the same enactment instead of any separate legislation. …

De-Identification: Guidance / Code of Conduct Approach

- Best known:
  - In Canada: IPC-Ontario's De-Identification Guidelines for Structured Data
  - Global: UK-ICO Anonymisation Guidance (currently being updated) or Article 29 WP Opinion on Anonymisation Techniques
- More detail: UK Anonymisation Network's Anonymisation Decision-Making Framework

- Standards:
  - ISO/IEC 20889 – Privacy enhancing data de-identification terminology and classification of techniques
  - ISO/IEC 27559 – Privacy enhancing data de-identification framework (in development)
  - CAN/CIOSC 100-3 – Data Governance – Part 3: Privacy enhancing data de-identification framework (in development)

See also: https://privacydocs.github.io/Deidentification/

De-Identification – Non-Identifiable Data

Are we only promoting de-identification?

- Consider C-11:

  39(1)(a) An organization may disclose an individual's personal information without their knowledge or consent if the personal information is de-identified before the disclosure is made;

  …

What about:

- **Data Synthesis?**
- **Secure Multi-Party Computation?**
- **Homomorphic Encryption?**

Artificial Intelligence

Background – Automated Decision-Making

GDPR Article 22: Automated individual decision-making, including profiling

1. The data subject shall have the **right not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the **right to obtain human intervention** on the part of the controller, to **express his or her point of view** and to **contest the decision**.

Background – Automated Decision-Making

But, a key question … what is “automated processing” (or automated decision-making)?

Article 29 Working Party – Guidelines on automated individual decision-making and profiling

> Article 22(1) refers to decisions ‘based solely’ on automated processing. This means that there is **no human involvement** in the decision process. … To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision.

Canada – **Directive on Automated Decision-Making** (largely included in C-11)

> [A]ny technology that either **assists or replaces** the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets.

Background – Categorizing AI

- OECD Framework for the Classification of AI Systems (February 22, 2022)
- Goals:
  - Promote a common understanding of AI by identifying features that matter most
  - Inform registries or inventories by describing systems and their basic characteristics
  - Support sector-specific framework by providing the basis for more detailed application of criteria
  - Support risk assessment by informing work towards developing a risk assessment framework and a common framework for reporting AI incidents
  - Support risk management by informing work on mitigation, compliance, and enforcement.
- Key dimensions:
  - People & Planet
  - Economic Context
  - Data & Input
  - AI Model
  - Task & Output

PEOPLE & PLANET	Criteria	Description
USERS	Users of AI system	What is the level of competency of users who interact with the system?
STAKEHOLDERS	Impacted stakeholders	Who is impacted by the system (e.g. consumers, workers, government agencies)?
OPTIONALITY	Optionality and redress	Can users opt out, e.g. switch systems? Can users challenge or correct the output?
HUMAN RIGHTS	Human rights and democratic values	Can the system's outputs impact fundamental human rights (e.g. human dignity, privacy, freedom of expression, non-discrimination, fair trial, remedy, safety)?
WELL-BEING & ENVIRONMENT	Well-being, society and the environment	Can the system's outputs impact areas of life related to well-being (e.g. job quality, the environment, health, social interactions, civic engagement, education)?
DISPLACEMENT	*{Displacement potential}*	*Could the system automate tasks that are or were being executed by humans?*
ECONOMIC CONTEXT	**Criteria**	**Description**
SECTOR	Industrial sector	Which industrial sector is the system deployed in (e.g. finance, agriculture)?
BUSINESS FUNCTION & MODEL	Business function	What business function(s) is the system employed in (e.g. sales, customer service)?
	Business model	Is the system a for-profit use, non-profit use or public service system?
CRITICALITY	Impacts critical functions / activities	Would a disruption of the system's function / activity affect essential services?
SCALE & MATURITY	Breadth of deployment	Is the AI system deployment a pilot, narrow, broad or widespread?
	{Technical maturity}	*How technically mature is the system (Technology Readiness Level –TRL)*
DATA & INPUT	**Criteria**	**Description**
COLLECTION	Detection and collection	Are the data and input collected by humans, automated sensors or both?
	Provenance of data and input	Are the data and input from experts; provided, observed, synthetic or derived?
	Dynamic nature	Are the data dynamic, static, dynamic updated from time to time or real-time?
RIGHTS & IDENTIFIABILITY	Rights	Are the data proprietary, public or personal data (related to identifiable individual)?
	"Identifiability" of personal data	If personal data, are they anonymised; pseudonymised?
STRUCTURE & FORMAT	*{Structure of data and input}*	*Are the data structured, semi-structured, complex structured or unstructured?*
	{Format of data and metadata}	*Is the format of the data and metadata standardised or non-standardised?*
SCALE	*{Scale}*	*What is the dataset's scale?*
QUALITY AND APPROPRIATENESS	*{Data quality and appropriateness}*	*Is the dataset fit for purpose? Is the sample size adequate? Is it representative and complete enough? How noisy are the data?*

AI MODEL	Criteria	Description
MODEL CHARACTERISTICS	Model information availability	Is any information available about the system's model?
	AI model type	Is the model symbolic (human-generated rules), statistical (uses data) or hybrid?
	{Rights associated with model}	*Is the model open-source or proprietary, self or third-party managed?*
	{Discriminative or generative}	*Is the model generative, discriminative or both?*
	{Single or multiple model(s)}	*Is the system composed of one model or several interlinked models?*
MODEL-BUILDING	Model-building from machine or human knowledge	Does the system learn based on human-written rules, from data, through supervised learning, through reinforcement learning?
	Model evolution in the field ML	Does the model evolve and / or acquire abilities from interacting with data in the field?
	Central or federated learning ML	Is the model trained centrally or in a number of local servers or "edge" devices?
MODEL INFERENCE	*{Model development / maintenance}*	*Is the model universal, customisable or tailored to the AI actor's data?*
	{Deterministic and probabilistic}	*Is the model used in a deterministic or probabilistic manner?*
	Transparency and explainability	If information available to users to allow them to understand model outputs?

TASK & OUTPUT	Criteria	Description
TASKS	Task(s) of the system	What tasks does the system perform (e.g. recognition, event detection, forecasting)?
	{Combining tasks and actions into composite systems}	*Does the system combine several tasks and actions (e.g. content generation systems, autonomous systems, control systems)?*
ACTION	Action autonomy	How autonomous are the system's actions and what role do humans play?
APPLICATION AREA	Core application area(s)	Does the system belong to a core application area such as human language technologies, computer vision, automation and / or optimisation or robotics?
EVALUATION	*{Evaluation methods}*	*Are standards or methods available for evaluating system output?*

AI: Standards Approach

UK AI Standards Hub (Announced January 12, 2022)

- Joint venture of the British Standards Institute and National Physical Laboratory, hosted by Alan Turing Institute
- Pilot tasks:
  - Growing UK engagement to develop global AI standards by bringing together information about technical standards and development initiatives in an accessible, user-friendly and inclusive way.
  - Bringing the AI community together through workshops, events and a new online platform to encourage more coordinated engagement in the development of standards around the world.
  - Creating tools and guidance for education, training and professional development to help businesses and other organisations engage with creating AI technical standards, and collaborate globally to develop these standards.
  - Exploring international collaboration with similar initiatives to ensure the development of technical standards are shaped by a wide range of AI experts, in line with shared values.

AI: Accountability Approach

- Emerging accountability tools:

- Canada's Algorithmic Impact Assessment tool
- AI Now Algorithmic Impact Assessment framework
- Dutch Platform for the Information Society Artificial Intelligence Impact Assessment

Roadmap for conducting the AIIA

Organisations who want to conduct the AIIA can follow the roadmap below. An explanation to this plan can be found in 'Part 2: Conducting the AIIA', page 35.

Step 1 — Determine the need to perform an AIIA

1. Is the AI used in a new (social) domain?
2. Is a new form of AI technology used?
3. Does the AI have a high degree of autonomy?
4. Is the AI used in a complex environment?
5. Are sensitive personal data used?
6. Does the AI make decisions that have a serious impact on persons or entities or have legal consequences for them?
7. Does the AI make complex decisions?

Step 2 — Describe the AI application

1. Describe the application and the goal of the application
2. Describe which AI technology is used to achieve the goal
3. Describe which data is used in the context of the application
4. Describe which actors play a role in the application

Step 3 — Describe the benefits of the AI application

1. What are the benefits for the organisation?
2. What are the benefits for the individual?
3. What are the benefits for society as a whole?

Step 4 — Are the goal and the way the goal is reached ethical and legally justifiable?

1. Which actors are involved in and/or are affected by my AI application?
2. Have these values and interests been laid down in laws and regulations?
3. Which values and interests play a role in the context of my deployment of AI?

Step 5 — Is the application reliable, safe and transparent?

1. Which measures have been taken to guarantee the reliability of the acting of the AI?
2. Which measures have been taken to guarantee the safety of the AI?
3. Which measures have been taken to guarantee the transparency of the acting of the AI?

Step 6 — Considerations and assessment

Step 7 — Documentation and accountability

Step 8 — Review periodically

AI: Accountability Approach

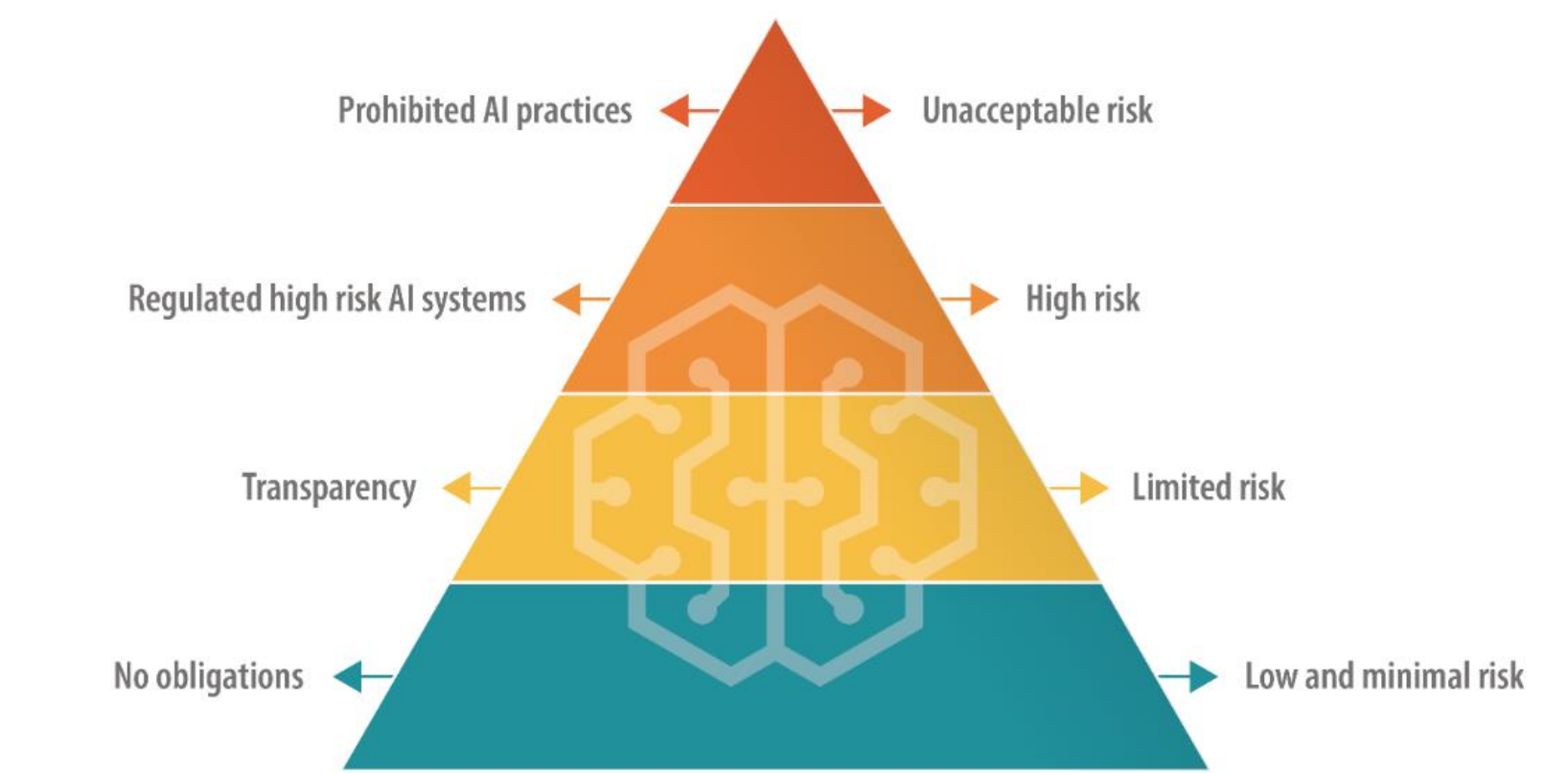
- US Algorithmic Accountability Act

[Key Definition: The term “automated decision system” means any system, software, or process (including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques and excluding passive computing infrastructure) that uses computation, the result of which serves as a basis for a decision or judgment.]

- In short: Any automated decision system developed for use in an augmented critical decision process must undergo an impact assessment.
- Impact assessment must consider (among other things):
  - Purpose, necessity and benefits of the system (compared to existing process)
  - Reviews of system performance, including demographic differences
  - Need for guardrails
  - Rights available to consumers
  - …

AI: Accountabilty Approach (cont'd)

- EU AI Act



EU AI Act – Prohibited Practices

- AI systems that deploy harmful manipulative 'subliminal techniques';
- AI systems that exploit specific vulnerable groups(physical or mental disability);
- AI systems used by public authorities, or on their behalf, for social scoring purposes;
- 'Real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, except in a limited number of cases.

EU AI Act – High Risk

- AI is High Risk if deployed as a safety component of a product, or deployed in the following areas:
  - Biometric identification and categorisation of natural persons;
  - Management and operation of critical infrastructure;
  - Education and vocational training;
  - Employment, worker management and access to self-employment;
  - Access to and enjoyment of essential private services and public services and benefits;
  - Law enforcement;
  - Migration, asylum and border control management;
  - Administration of justice and democratic processes.

EU AI Act – High Risk Requirements

- Establish a risk management system that applies throughout the lifecycle of the system (Article 9)
  - “The risk management measures … shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse.”
- Data Governance (Article 10)
  - “High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the [stated] quality criteria.”
- Event logging (record keeping) (Article 12)
- Transparency (Article 13)
  - “High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system’s output and use it appropriately.”
  - “High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.”
- Human Oversight (Article 14)
  - High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

EU AI Act – High Risk Requirements

- Accuracy, Robustness, Cybersecurity (Article 15)
  - “High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.”
- Providers of High Risk AI systems must also undergo a conformity assessment, register their system in an EU-wide database before putting them into market, and many other requirements.
  - High-risk AI systems used for biometric identification would require a conformity assessment by a “notified body”

AI: Principles and Ethics Approach

- OECD AI Framework:
  - **Inclusive growth, sustainable development and well-being**: This Principle highlights the potential for trustworthy AI to contribute to overall growth and prosperity for all – individuals, society, and planet – and advance global development objectives.
  - **Human-centred values and fairness**: AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and should include appropriate safeguards to ensure a fair and just society.
  - **Transparency and explainability**: This principle is about transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes.
  - **Robustness, security and safety**: AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.
  - **Accountability**: Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the OECD's values-based principles for AI.

See also: AIEthicist list of Frameworks, Guidelines, Toolkits; Principles

In Canada: See for example Ontario's Beta principles for ethical use of AI and data enhanced technologies in Ontario

- Transparent & explainable; good and fair; safe; accountable and responsible; human-centric; sensible and appropriate.

Data Subject Rights

The Eight (or Nine, or Ten) GDPR Rights

- Right to be Informed (Article 13 / 14)
- Right of Access (Article 15)
- Right to Rectification (Article 16 / 19)
- Right to Erasure ('Right to be Forgotten') (Article 17 / 19)
- Right to Restriction (Article 18 / 19)
- Right to Data Portability (Article 20)
- Right to Object (Article 21)
- Rights related to Automated Decision Making and Profiling (Article 22)

(and, depending on who's counting, Right to Notification and/or Right to Withdraw Consent)

In Canada?

Under PIPEDA – and noting that much of this is subject to debate / interpretation:

☑ Right to be Informed (Article 13 / 14)

☑ Right of Access (Article 15)

☑ Right to Rectification (Article 16 / 19)

☒ Right to Erasure ('Right to be Forgotten') (Article 17 / 19)

☒ Right to Restriction (Article 18 / 19)

☒ Right to Data Portability (Article 20)

☒ Right to Object (Article 21)

☒ Rights related to Automated Decision Making and Profiling (Article 22)

A comparator: Philippines

Implementing Rules and Regulations of the Data Privacy Act of 2012

Rule VIII: Rights of Data Subjects

- Right to be informed
- Right to object
- Right to access
- Right to rectification
- Right to erasure or blocking
- **Right to damages**
  - The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.
- Right to data portability

Also speaks to transmissibility of rights; limitations on rights (i.e. rights are not applicability is data is used only for scientific / statistical research and no decisions are taken regarding the data subject, and in the context of criminal investigations).

For more info: NPC Advisory 2021-01, on Data Subject Rights

Right to Erasure (Right to be Forgotten)

EU Article 17

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- Data are no longer necessary
- Data subject withdraws consent
- Data subject objects
- Data have been processed unlawfully
- Requirement for erasure for compliance with a legal obligation;
- Data was collected about a youth per Article 8(1)

Where the data has been made public, the controller shall take reasonable steps to inform other controllers of the erasure request.

EU Article 17

... unless processing is necessary:

- For exercising the right of freedom and information
- For compliance with a legal obligation
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest
- For the establishment, exercise or defence of legal claims.

Philippines Right to Erasure or Blocking

The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon **discovery and substantial proof** of any of the following:
   (a) The personal data is incomplete, outdated, false, or unlawfully obtained
   (b) The personal data is being used for purpose not authorized by the data subject;
   (c) The personal data is no longer necessary for the purposes for which they were collected;
   (d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
   (e) The personal **data concerns private information that is prejudicial to data subject**, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
   (f) The processing is unlawful;
   (g) The personal information controller or personal information processor violated the rights of the data subject.

2. The personal information controller may notify third parties who have previously received such processed personal information.

Quebec Bill 64 – The first explicit de-indexing law?

28.1: The person to whom personal information relates may require any person carrying on an enterprise to **cease disseminating that information or to de-index any hyperlink attached to his name that provides access to the information** by a technological means, if the dissemination of the information contravenes the law or a court order.

The person may do likewise, or may require that the hyperlink providing access to the information be re-indexed, where the following conditions are met:

1. the dissemination of the information causes the person concerned **serious injury** in relation to his right to the respect of his reputation or privacy;
2. the **injury is clearly greater than the interest of the public** in knowing the information or the interest of any person in expressing himself freely; and
3. the **cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary** for preventing the perpetuation of the injury.

Quebec Bill 64 – The first explicit de-indexing law?

In assessing the criteria set out in the second paragraph [injury vs. public interest], the following, in particular, must be taken into account.

1. the fact that the person concerned is a **public figure**;
2. the fact that the information concerns the person **at the time the person is a minor**;
3. the fact that the information is **up to date and accurate**;
4. the **sensitivity** of the information
5. the **context** in which the information is disseminated;
6. the **time elapsed** between the dissemination of the information and the request made under this section; and
7. where the information concerns a criminal or penal procedure, the **obtaining of a pardon** or the application of a restriction on the accessibility of records of the courts of justice.

Google stats on de-indexing

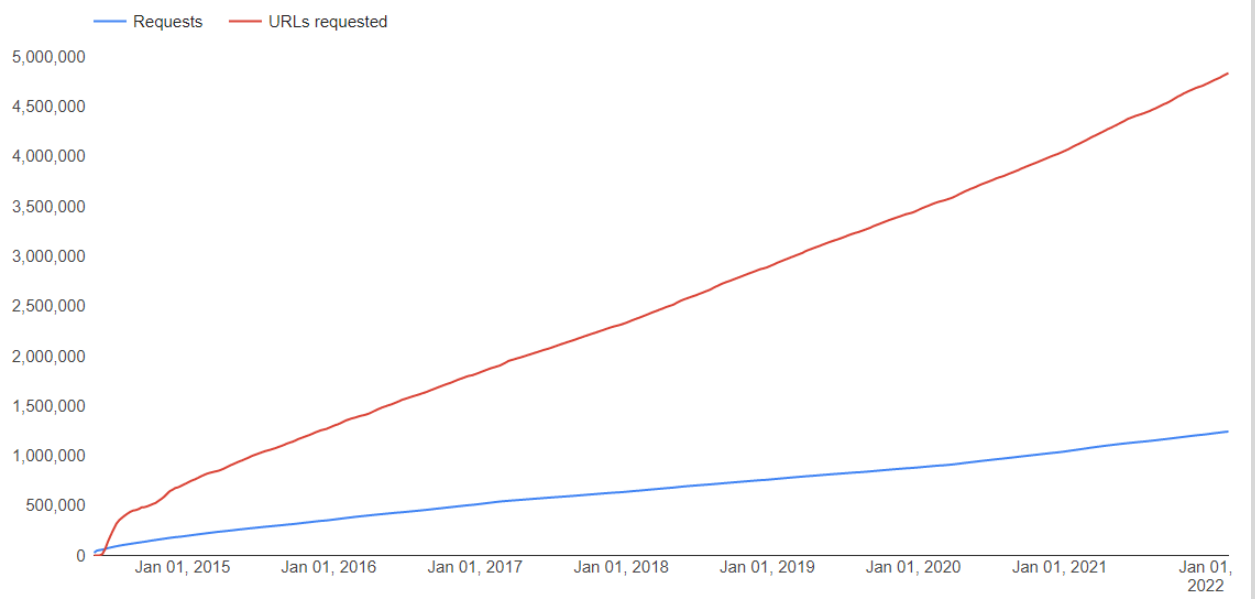
Requests to delist

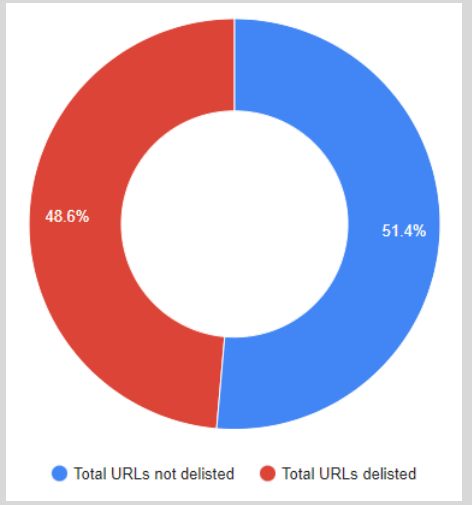
1,241,409

URLs requested to be delisted

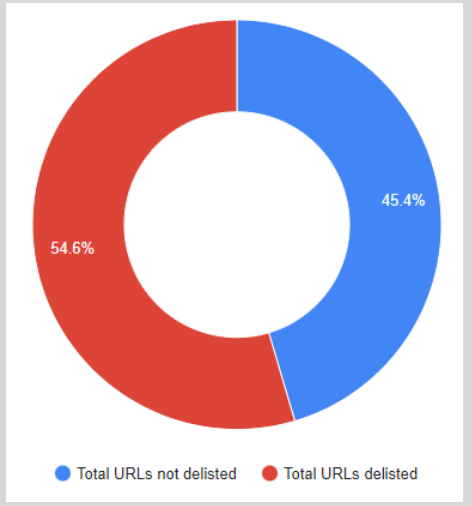
4,832,545

Requests received over time





All-time



Since 2020

Right to Data Portability

Article 20 – Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, **which he or she has provided to a controller**, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- The processing is based on consent or a contract; and,
- The processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Data mobility under C-11

Mobility of Personal Information - Disclosure under data mobility framework

72 Subject to the regulations, on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations.

Data mobility frameworks

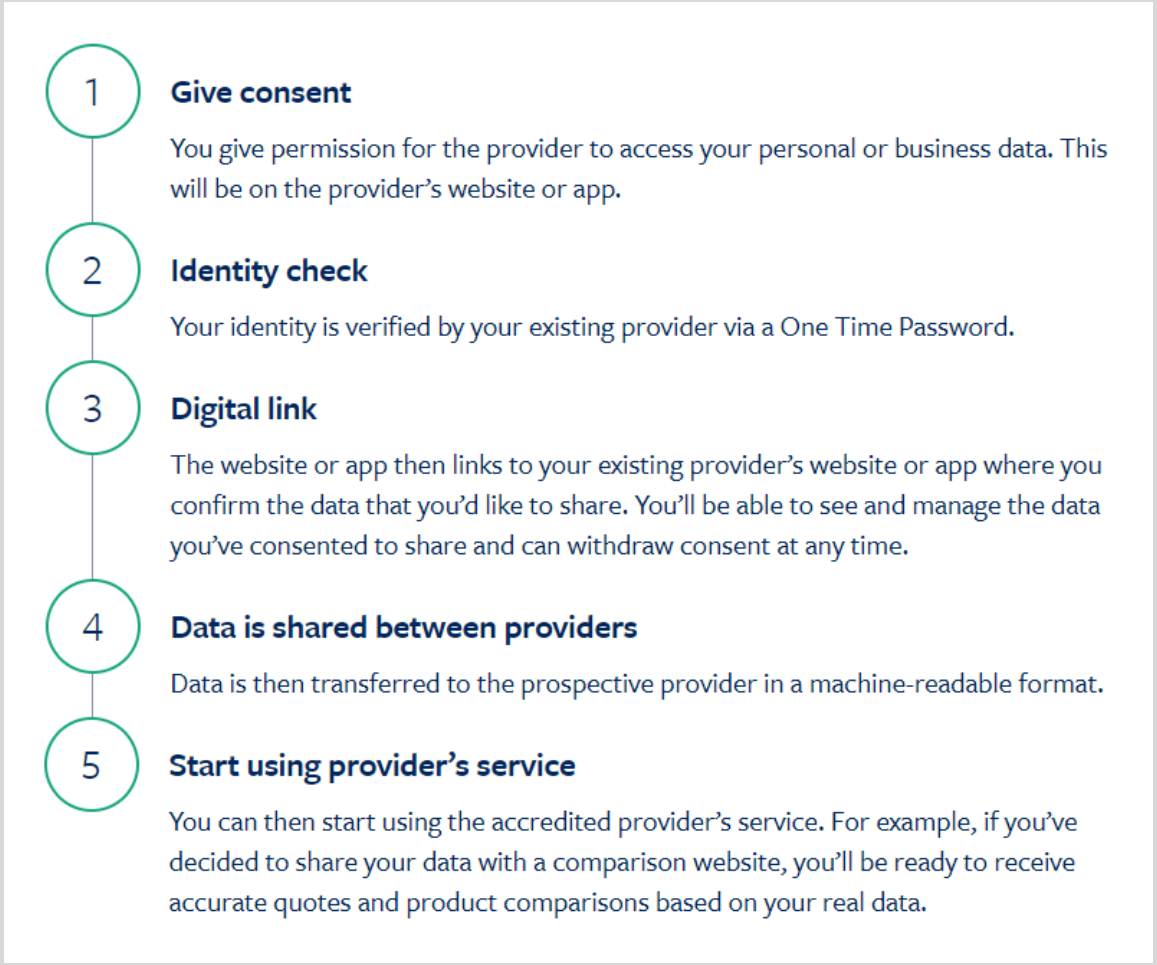
120 The Governor in Council may make regulations including regulations respecting data mobility frameworks that provide for

- safeguards that must be put in place by organizations to enable the secure disclosure of personal information under section 72 and the collection of that information, and
- parameters for the technical means for ensuring interoperability in respect of the disclosure and collection of that information;

Governor in Council may also specify what organizations that are subject to a data mobility framework.

Australian Consumer Data Right

- Established as an amendment to the Competition and Consumer Act (Part IVD); further defined in the Competition and Consumer (Consumer Data Right) Rules 2020
- Overseen by the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC)
- Currently applies in financial sector; energy sector next
- Key aspects:
  - Development of consumer data standards
  - Accreditation of service providers



End Part 4.